IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, INC.,)
)
Plaintiff,)
v.) Civil Action No.:
) 2:18cv94
CISCO SYSTEMS, INC.,)
)
Defendant.)

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia
May 6, 2020

Volume 1A
Pages 1-93

BEFORE: THE HONORABLE HENRY C. MORGAN, JR.
United States District Judge

Appearances: (Via Zoomgov Video)

KRAMER LEVIN NAFTALIS & FRANKEL, LLP
By: PAUL JOSEPH ANDRE
Counsel for Plaintiff

DUANE MORRIS, LLP
By: LOUIS NORWOOD JAMESON
MATTHEW CHRISTOPHER GAUDET
-- **and** --
DAVIS POLK & WARDWELL
By: NEIL HARVEY MacBRIDE
Counsel for Defendant

P R O C E E D I N G S

(Proceedings commenced at 10:07 a.m. as follows:)

COURTROOM DEPUTY CLERK: Civil Action No. 2:18cv94, Plaintiff Centripetal Networks, Inc. v. Cisco Systems, Inc.

For the plaintiff, Mr. Noona, Mr. Andre, are you ready to proceed?

MR. NOONA: We are, Your Honor.

THE COURT: For the defendants, Mr. Jameson, Mr. Carr, are you ready to proceed?

MR. JAMESON: We are, Your Honor.

THE COURT: All right. We're conducting this trial by remote video under the Zoom --

MR. ANDRE: The Court is muted.

THE COURT: Can you hear me now?

MR. ANDRE: Yes, Your Honor, we can hear you.

THE COURT: All right. We're conducting this trial by video on the Zoom platform, which is the one that's been approved by the U.S. Courts federal court system, and we're going to follow as closely as is possible to do under the circumstances to the regular rules of the court.

The Court was very anxious to try this trial because it involves important issues of intellectual property which have a potential impact on programs that could be of national

importance for the country.

We are conducting this trial openly insofar as we can; that is, it's open to the public on audio, not on video. The people watching on audio should mute themselves; otherwise, if you are just talking for any reason it'll go over the audio to everybody else who is on it. So you should mute yourselves whenever you're watching it.

Also, the rules of court apply the same as if you were sitting in the court or if you were ordered by the Court to be separated. By that I mean no one should be watching on the video if they are going to be a witness in the case. If you watch any part of the case you would be violating the Court's order if you discussed anything you saw -- well, you wouldn't see -- anything you heard on the audio with any other witness in the case. So the public is welcome to listen to the video on mute, but you're not admitted to discuss your testimony with anyone or discuss what you've observed with anyone who may give testimony in the case.

We will probably have more recesses than we ordinarily have due to the logistics of trying to keep everyone separated. And if someone needs a recess, you can ask for it. If there's any problem with the technology, we'll of course recess until we can resolve that.

The Court's schedule will normally be to convene at 10:00 in the morning and take a recess in the middle of the

morning somewhere around 11:30, depending upon where we stand with witness testimony at that time, and we'll normally adjourn for lunch at 1:00 and resume at 2:00. I assume we can all handle a one-hour luncheon recess. It's sometimes difficult when everyone has to leave the courtroom and go out and get lunch and come back, but under these circumstances, I assume everyone's okay with a one-hour recess for lunch.

In the afternoons, we will resume at 2:00 and adjourn at 4:00. We will not take a recess in the afternoon unless it's necessary for handling the technology with a witness.

One matter that I wanted to discuss before we begin is the fact that there are not going to be any time limits. It's frequently the case in patent litigation that the judge imposes time limits on each side. We're not going to do that in this case because I think that would be premature to do that until we learn how proceeding in the manner that we are will affect the progress of the trial. So unless the Court rules otherwise, we're not operating under time limits.

The issue also arose about the findings of fact and conclusions of law. In retrospect, I can understand why counsel furnished such detailed documents, and the question is how can we try to make practical use of the findings of fact and conclusions of law in the case. And I believe that the best thing that we can do is have the points of law that the proponent of each witness intends to present made available to

the Court before the witness testifies. It may not be possible -- well, I'm sure it's not possible to do that today -- but what I'm thinking is we have an exhibit book for each witness, and what I want to do starting tomorrow is to have a list of the points that each side wishes to present through the witness. In other words, we'll take the findings of fact as they apply to each individual witness. I'm sure that counsel has prepared something of that nature for each witness anyway. I'm not suggesting that we have to outline every single question for each witness, but I am suggesting that we can make an outline of each factual scenario that you wish to present through each witness and have it delivered to the Court prior to the witness's testimony. It can be immediately prior. And I would confine it to four pages for the proponent and two pages for the cross-examination. There's no obligation that this list be made available to opposing counsel until the witness is called, or to the Court. Same for cross-examination: You don't have to hand it over until you actually begin your cross. And the cross, as I say, will be limited to two pages, doubled-spaced. And I say double-spaced because one of the attorneys made the observation that the Court may want to annotate the findings of fact in the course of the trial, which I think is a good idea. And if it's double-spaced, I can annotate and make my annotations on those lists themselves as they're supplied to me.

Now, if counsel wanted to supply that to the Court or opposing counsel sooner than I suggested, that's fine, if you can agree on that. But I would like it made available to the Court prior to the witness's testifying. I don't think that will be very burdensome because I think most attorneys make an outline of what they want to present through each witness in advance anyway. So you can just turn those outlines in to something that you can deliver to the Court and to opposing counsel.

MR. JAMESON: Your Honor, this is Woody Jameson. Could I ask a follow-up question on that now?

THE COURT: You may.

MR. MacBRIDE: Would you actually like this summary for us to be trying to identify the specific findings or conclusions of law by number, or is it more summary fashion?

THE COURT: I would present them in the form of numbered paragraphs. Now, trying to coordinate them with the numbered paragraphs in your conclusions of law may be a difficult burden, particularly in the short-term, so I don't think that's necessary. Just put them in numbered paragraphs, and we can worry about coordinating the numbered paragraphs with the findings of fact later.

MR. JAMESON: And would you anticipate that at the conclusion of trial it will be of benefit to the Court that both sides provide you record cites to their proposed findings of

fact and conclusions of law?

THE COURT: Yes, I think it would be.

All right. Is there anything further?

MR. ANDRE: Nothing from Centripetal, Your Honor.

MR. JAMESON: Your Honor, it was my understanding -- and I don't know whether you want to take this up now or before we start the actual presentation of evidence -- but I think that there was some, just one or two disagreements about witness presentation and some exhibits that may come up as early as today.

THE COURT: You mean motions *in limine*?

MR. JAMESON: With your permission, I would turn it over to Neil MacBride. He was going to handle the issues for Cisco to at least preview them to you and figure out whether you want to deal with them now or later.

THE COURT: All right.

MR. MacBRIDE: Good morning, Your Honor. Neal MacBride for Cisco Systems, Inc.

THE COURT: Good morning.

MR. MacBRIDE: Your Honor, we just wanted guidance before we get underway with the tech tutorial and the openings. There are a couple of issues that have not yet been resolved between Centripetal and Cisco, mostly the calling of live witnesses, the playing of video depositions that have been designated by both parties in the nature of those issues. And

very happy to wait until the trial starts to address them at that point, but just wanted the Court to know that there are a couple of housekeeping matters that we would like to discuss at some point.

THE COURT: No, we can discuss them now. Counsel has worked very hard to come up with what I think is an excellent outline of how you're going to handle the witnesses, and it appears that your suggestions comport with the Rules, Federal Rules, as well as the Local Rules. So I think every one that's in there at this point is helpful and proper. But if you have any areas of disagreements, we might as well get those resolved up front.

MR. MacBRIDE: Thank you, Your Honor. I believe that there are essentially three outstanding disputes at the moment. I'm happy to take them one at a time if the Court would like to hear from Mr. Andre, but the first issue, Your Honor, involves the issue of mutually identified live witnesses. Fact witnesses. And certain witnesses have been identified for live testimony, in fact witnesses by both parties, for example Mr. Rogers, Mr. Steve Rogers, Mr. Sean Moore will be testifying later this week for Centripetal. These same individuals, Your Honor, are fact witnesses which Cisco could call in its case-in-chief as well. And so in the view of Cisco, our proposal to Centripetal was, rather than burdening the Court and the witnesses with multiple appearances, we suggested that, for

example, Cisco be allowed to question Mr. Rogers or Mr. Sean Moore this week at the conclusion of their direct testimony with any of the topics that we would raise in our case-in-chief, and then of course Centripetal would be allowed to perform redirect examination of that witness during their sole appearance in view of Cisco's examination. And as we understand it, Centripetal is opposed to the request and instead would like witnesses to be recalled by the other party in its case-in-chief rather than just appear a single time.

MR. ANDRE: Your Honor, this is Paul Andre. We have told Cisco if they wanted to call our witnesses in their case-in-chief we'll make them available. It's no burden on witnesses. We're doing this by video. Mr. Rogers is doing it from his home in New Hampshire, so that's not a problem. We're going to be presenting Mr. Rogers, the founder of the company, right after we finish the opening statements this afternoon. And what we probably have, with Cisco's proposal, is that they intend to take him on not only cross-examination when we take the examination on, but also our problem they want to take him on. We have not been provided exhibits in advance like we have to do if they have taken him on their case-in-chief as a direct witness. It would be a complete surprise to us.

So what we're saying is, we're not going to take any of the Cisco witnesses live in our case-in-chief. We'll play a deposition of their witnesses. We've taken depositions. We're

going to submit written testimony in the form of these deposition summaries and clips. So they want to go in and essentially disrupt our case other presentation of our case by going in and doing what essentially is their case-in-chief in the midst of our fact witnesses.

So there's two issues. One is it's procedurally not appropriate. Two, it's complete surprise because they have not given us any notice as to what they want to examine the witness on in their case-of-chief, and they have not given us the exhibits like we would normally get. For example, we gave them our exhibits that we're going to use for Mr. Rogers or Mr. Moore -- Dr. Moore, three days in advance and et cetera.

THE COURT: Well, one difficulty with presenting him one time only would be part of the presentation would be cross-examination of some witnesses and part of it would be direct examination. I mean, the president of your company would certainly qualify as an adverse witness who could be led, but there may be other fact witnesses in a different situation. Unless there's a problem with the availability of the witness, I think it would be better to call such witnesses as they have been mentioned and then recall them if necessary instead of trying to do both of them at once. I would like to adhere as close as possible in this proceeding as we would if we were doing it in the courtroom, and I think that's the way we would do it if we were in the courtroom. So I think we should stick

with that.

MR. ANDRE: Thank you, Your Honor.

THE COURT: All right.

MR. MacBRIDE: The second issue, Your Honor, if I may be heard on that, relates to the consolidation of third party witness deposition testimony. So in other words, there are certain third-party witnesses whose deposition testimony have been affirmatively designated by both Centripetal and Cisco. So for example, Centripetal may play the deposition transcript in the next few days of some of these third-party witnesses. And we raised with Centripetal our suggestion and provided to the Court that rather than providing the Court with overlapping -- rather than burdening the Court, excuse me, Your Honor, with overlapping testimony, we would request that the party's affirmative designations and the counter-designations designation be played together at the same time. And so in practice this would mean that both Cisco and Centripetal can each play their affirmative designations on the same day as well as the respective counter-designations rather than waiting for their case-in-chief and have a repeat of deposition video transcript.

THE COURT: Well, wouldn't that be -- let's assume the witness was in court instead of testifying by deposition. Wouldn't a third-party witness be called by one side and examined and then cross-examined by the other side? Isn't that

what happened in the deposition?

MR. JAMESON: That's correct, Your Honor. We had thought, though, that there could be efficiencies for the Court to have the benefit of having them at the same time.

THE COURT: Well, that seems to be logical. In other words, if the witness were here in court, the witness would be presented by the proponent and then cross-examined. We wouldn't present the witness and then bring a witness back for cross-examination, we would do the whole thing at once. Why shouldn't we do the whole thing at once, Mr. Andre?

MR. ANDRE: Your Honor, we agree with that. We agree that the cross-examination -- the counter-designations for the portions that were designated, the cross-examinations, as it were, is appropriate. 100 percent. What they want to do though is go in and put in what they would have wanted put in in their direct testimony. Just what we were talking about with the live witnesses. They want to add in their testimony as well. Now, I don't think it's going to be an issue. Most of this is going to be submitted in the form of written testimony to the Court for submission. But if it comes up, I think we can deal with it. But it's, I don't think it's appropriate for them to put in -- they want to examine the witness themselves. Like in many instances they subpoenaed the third party, but they want to put in their portion they would like to put in --

THE COURT: You mean there were two depositions of

people?

MR. ANDRE: There was -- a third party would be in a deposition, would be the subpoenaed party, then the opposing party would also take it as well. So it wasn't straight cross-examination.

THE COURT: In other words, they brought up matters in cross that were not brought up in direct?

MR. ANDRE: That's correct, Your Honor.

THE COURT: Well, that's something that frequently happens in the examination of a witness. I think in that instance it would be better to just present all of the deposition testimony at once. If defense counsel went beyond cross-examination and brought up matters that weren't brought in direct, meaning that they couldn't cross-examine them, they just wouldn't be allowed to cross-examine them. But I think we ought to hear it all at one time in that instance. I'm trying to do what we would do if we were in court. That's how we would to it if we were in court.

MR. ANDRE: Your Honor, that was our point. If we had the direct examination, anything they cross-examinationed on would be completely appropriate, or even further testimony that was relevant to that testimony is fine, but if they go outside of the scope of direct, we think that would be inappropriate. If Your Honor wants us to play all of it, we can do that as well.

THE COURT: Well, I think we just play all of it. That's what we would do if the witness were here in court, I would just say if you're going to go beyond what was in direct, you're making them your witness, and you can't cross-examine them.

Now of course when it comes to exhibits to be used with the witness, they would have to be supplied in the normal, in accordance with what counsel has agreed on.

MR. MacBRIDE: Thank Your Honor.

Your Honor, the final issue is one -- it's simply a objection that Centripetal has raised to a proposed exhibit that -- excuse me, that Cisco has raised. It's a direct exhibit that would be used with Mr. Steven Rogers and proposed by Centripetal. We've not been able to have a meeting of the minds and so we continue to disagree. We have an objection to the document. And we can bring that up now and discuss it, Your Honor, or at the time of Mr. Rogers' direct. Just wanted to let you know that that's one open issue that remains at this point.

THE COURT: Well, I think we'll take that up when he takes the stand.

MR. MacBRIDE: Very good.

That was it from Cisco, Your Honor. Thank you.

THE COURT: All right. Well, the first -- Brandan?

(Court and law clerk conferred.)

THE COURT: One thing I'll bring up while we have a

pause here, for the purpose of those observing the matter by audio, is that we frequently have bench conferences to decide issues of evidence. So it may be necessary during the course of the proceeding to turn the audio off when we're having what would amount to a bench conference in the course of trial. So those people who were observing via audio, I just wanted to let you know that if we were all in open court I would just ask counsel to come up to the bench and we would turn the microphones off so that nobody could hear what we were talking about. Issues may come up in the course of the trial where I would have the equivalent of a bench conference, and what I'll do in that situation is I'll just turn the audio off until we complete whatever the matter is that we're discussing confidentially.

All right. I have the documents from my clerk that I was looking for, so if there are no further issues, we can begin with the presentation on behalf of the plaintiff.

MR. ANDRE: Your Honor, this is Paul Andre for Centripetal, the plaintiff.

As the Court ordered, both sides will be presenting a technology tutorial. The parties have agreed that each of the experts for Centripetal and Cisco will present Your Honor with a general tutorial of the technology, not in advocacy role, but just to give the Court a background, and there will be no cross-examination. Thereafter, we'll do the opening statement.

THE COURT: All right.

MR. ANDRE: With that, Centripetal would like to call Dr. Nenad Medvidovic to the stand.

THE COURT: All right. Go ahead.

MR. GAUDET: Your Honor, this is Matt Gaudet for Cisco. I just wanted to let you know, with respect to the tutorials, I'll be the person handling this on behalf of Cisco. I'll be completely silent while Mr. Andre would offer that tutorial, but I wanted the Court to know who the face on the screen was, Your Honor.

THE COURT: Okay.

MR. ANDRE: Your Honor, at this point, before we give the tutorial, the parties have agreed that the only fact witnesses that can sit through the tutorials are the corporate representatives pursuant to the pretrial order. So I just would like to remind any individual fact witnesses coming on through video or through audio to now drop off the line if that's okay with Your Honor.

THE COURT: Okay.

MR. ANDRE: Thank Your Honor.

Lori, are we going to swear in the tutorialists?

COURTROOM DEPUTY CLERK: Do you want him to be sworn?

THE COURT: Yes.

NENAD MEDVIDOVIC, having been duly sworn, was examined and testified as follows:

MR. ANDRE: May it please the Court. May I begin?
THE COURT: You may.
MR. ANDRE: Thank you, Your Honor.
TECHNOLOGY TUTORIAL OF PLAINTIFF
BY MR. ANDRE:
Q. Dr. Medvidovic, good morning.
A. Good morning.
Q. Why don't we start by letting the Court know who you are. Can we just see the slide of your qualifications?
A. Sure. I am a professor of computer science at the University of Southern California. I have been at USC since January of 1999. Before that I got a Bachelor's degree, a Master's degree and a Ph.D. First degree was from Arizona State University in computer science and engineering, the latter two were from the University of California at Irvine in information and computer science.
THE COURT: How do you spell your name, sir?
THE WITNESS: The first name is spelled N-e-n-a-d.
THE COURT: N-e-n-a-d.
THE WITNESS: That is correct, Your Honor.
The last name is M-e-d-v-i-d-o-v-i-c.
THE COURT: Medvidovic. Is that right?
THE WITNESS: Medvidovic. But yes, close.
MR. ANDRE: Your Honor, just for the record, all of his students and we call him Neno, because that name's a

mouthful.

THE COURT: All right.

COURTROOM DEPUTY CLERK: What happened?

LAW CLERK: The Judge dropped.

THE COURT: What happened? Do we know?

COURTROOM DEPUTY CLERK: Hold, please.

THE COURT: Well, everything went blank. We had two hearings yesterday without a hitch. So hope nobody's put malware in the system.

MR. ANDRE: Between the two parties, we have enough experts, we should be able to fix this.

THE COURT: I hope so.

So if we can just get the doctor back on the screen?

MR. ANDRE: Your Honor, because Dr. Medvidovic will be coming back later in the case, he's just doing the tutorial now, we'll expand on his credentials a little more later, but for now we'll just go with the presentation if that's okay with Your Honor.

THE COURT: That's fine.

BY MR. ANDRE:

Q. Dr. Medvidovic, could you describe the three types of devices found in computer networks we'll be focusing on in this case?

A. Yes. Let me see if I can control -- it doesn't look like I have the control. The three kinds of devices I'll overview

briefly over the next several minutes are switches, routers and firewalls. And we'll talk about each one of those in turn.

Q. Are these the three major devices you find in most computer networks?

A. Yes. These are the three kind of principle devices that comprise computer networks.

Q. Okay. Why don't we start off with switches.

THE COURT: Switches, routers and?

THE WITNESS: Firewalls.

THE COURT: Firewalls, okay.

BY MR. ANDRE:

Q. Start off with switches.

A. Sure. So the way to think about switches is similar to how a telephone switchboard operator worked back over half a century ago at this point, where there would be a call coming in, in this case from parents who want to speak to their daughter, they would provide the operator with the number, and then the operator would do the appropriate connection on the switchboard and eventually the parents could speak to their daughter. And in a sense, that is how computer switches work except that they don't connect people, and also they have to do things in much greater volumes than a human phone operator would have been able to do.

So this is what a modern-day switch box on a computer network looks like. It would connect things like a computer

with a printer, or a computer with another computer and so on.
    And what you see here, Your Honor, in the middle of this slide, is the schematic computer engineering symbol for a switch. So whenever you see this rectangle with those little shapes inside of it, that's what a switch is essentially represented as.
Q. Could you go back one slide, Dr. Medvidovic?
    So the switch box itself, all those little things in the back, are those just different ports for the plugs to go into it?
A. Those are the -- exactly. Those are the different ports. We call them plugs. And their shaped is exactly like the shape on that schematic that's coming up on the next slide that we just saw a second ago. This is why they're represented that way, because the network plugs look like those little shapes.
    So what switches allow us to do is build, for example, a whole network or a small business network. They basically allow us to hook together some number of devices that are reasonably close to one another physically. So when we do this, we create this network. In this case we're showing three computers, two printers, there could be fax machines, whatever else you might have on that network. And now everything is controlled, all the interaction between those different devices goes through that switch.
Q. And do switches have to be local? Do they all have to be

in the same building?

A. The devices themselves could be in a single location. They could also be on a -- in single building, for example, like the courthouse that Your Honor is in right now, or they could connect devices across, let's say, a company campus.

MR. ANDRE: All right. Unless Your Honor has any questions about switches, let's go to the next major computer device in a network: Routers.

A. Computer routers are the second major device that makes up a network. And unlike switches, which are like those phone switchboards, the way to think about a router is like a dispatcher. So for example here, we have an ambulance dispatcher, and what the router will do is it'll dispatch, in the real-world scenario that we're using here, a paramedic vehicle from Location A to Location B, and possibly advise them on what route to take so they can get there as quickly as possible. And that's essentially the job of a computer router, except of course it's routing computer data rather than routing humans inside of vehicles.

And the way a router is represented is with this symbol that looks like a hockey puck with arrows on it. That's just the computer engineering symbol that computer engineers use to represent the router.

What the router does, is it decides how to take the data that's coming in and route it in an optimal way to wherever it

needs to go so that it gets there as fast as possible. So here we're showing this U.S. Postal Service packet, which we'll talk about in a second, to represent computer data, and what the router does is essentially decides where it needs to go after it is sent.

Q. Does the router use the same route every time data packets are sent or does it pick the best route?

A. The routers are constantly trying to figure out, based on the current state of the network, which paths might be more clogged than others. So it's exactly trying to figure out what the best way of getting packets from Point A to Point B is. Meaning that between two different points in time, it could choose different routes and readjust and always try to do the best that it can based on the current status of the network.

Q. How do routers fit into the network structure?

There it is.

A. There we go. So this is basically how computer networks end up getting built. What you have in these boxes off to the sides are the small networks created by switches, those very local networks, and then what the routers do is they connect those networks into even larger networks. And now we're showing here schematically these packets of data traveling around, and the router figuring out where they need to go.

Now, this is still a relatively small network, but this can then expand, because you can have more routers connecting other

small networks and on and on and on, so that you can create nationwide networks or today's Internet, which basically is global.

MR. ANDRE: So unless Your Honor has any questions about routers, why don't we go to the third --

THE COURT: What did you mean by saying the word "mobile"?

THE WITNESS: I said "global", Your Honor.

THE COURT: Oh, "global". Excuse me. All right.

BY MR. ANDRE:

Q. We'll move to the third type of device we'll be talking about in this tutorial: The firewall. What is a firewall?

A. A firewall, just like in the real world in a hotel or a large office building, it's there for protection. So it's literally a wall between you and wherever there might be some sort of danger. In the case of a physical building it could be the actual fire, obviously. So if we go to the next slide, we're going to be presenting or representing firewalls with this brick wall with this flame symbol on it, and this flame symbol in particular is typically the computer engineer's chosen way of representing a firewall.

Q. What does the firewall do?

A. Basically a firewall takes some sort of a local network like what you see up there in the upper right side, and whenever data arrives from the outside from some sort of server on the

Internet, the firewall monitors that data, inspects it, and can do various things. Can decide what to do with it. So it establishes this barrier between the network you would like to protect and the outside world.

Q. So the web server in this example is the outside world, that's the Internet, and on the right side is your private network?

A. The web server could be anything that you're trying to get data from on the open Internet. The example we can maybe use to today is something like ESPN.com. So any data you try to see or retrieve from the ESPN servers would be on that web server. And that data would travel to you, but before it gets to your computer, it would first go through this firewall, and the firewall may decide to permit that data to go through because it does not violate any policies or rules that you may have for the firewall. Alternatively, the firewall may decide to block the data if the traffic is unauthorized. So for example, it could be in a company where the company policy is you can't watch sports during work hours. So in that case, that data from ESPN would be dropped at the firewall and never arrive to you.

Q. So how do all the firewall, routers and switches, how do they then fit into an entire network structure?

A. So this is a very simplified view of what a computer network may look like, obviously. It only has one printer, two computers, a couple of switches, one router and a firewall. But

you could imagine literally tens of thousands of these in a very large network working together, essentially. As we spoke before, the switches are there to connect mostly local devices, the routers are there to connect those small networks enabled by the switches, and then the firewalls sit there on the edge of a network to inspect the data, apply various rules to figure out what data may go through, what data may be dropped, and so on.

And then of course everything beyond the firewall on the left-hand side, that would be sort of the open Internet where whatever the organization is is not really able to control what happens. So what you try to do is you try to, in a way, protect things on the right-hand side of this firewall.

Q. So traditionally firewalls did serve some security function. Did -- in traditional networks do routers and switches have a security function?

A. Traditionally it was assumed that the security is going to be handled primarily at the firewall and the routers and the switches were there to ensure that the data gets to their destination as quickly as possible. So in a way, one way to think about it in traditional older networks, firewalls would focus on security, routers and switches would focus on performance and speed.

Q. Now, we're going to hear some other concepts in this case, and one of them is network packets. That's a big issue here. And you've shown a network packet represented as a Priority Mail

box that goes through the Postal Service. Could you describe what are the different components of a network packet?

A. Absolutely. So when you go to a server such as ESPN.com, and let's say you want to retrieve a video of the highlights of a football game that took place last Sunday -- well, there was in this case no football game last Sunday, of course -- but in a regular scenario there presumably would be during the season -- that video would not arrive from the server to your computer in a single chunk, because that could be a lot of data and it would be incredibly inefficient, and that's not how computer networks work.

What happens is that that video gets sliced up into a very large number of relatively small packets, and those are called data packets. And each one of those packets has two different parts. One of them is what we're representing here as the mailing label. And that basically has some header information; for example, it tells you what is the size of this particular packet, which packet in the ordering of all of the packets for that particular video it is. So it could be Packet 327, so that whoever is going to be reading this knows that Packets 326 and 328 need to be composed around that packet to get the actual video stream. It'll have the source of the packet, whoever sent it; it'll have the destination, where it's supposed to go; and possibly some other information as well. And that could be thought of as the, essentially a mailing label in a U.S. Postal

Service package.

Q. And what is the actual content of the video? What's that called?

A. Exactly. So the other thing that we need to worry about in a data packet in addition to that mailing label thing is the contents of the actual data. So the chunk of the video that is getting passed from ESPN.com to your laptop, and that's called the payload. And that, here, we are representing as the data that would actually -- the contents that would actually go inside of this box. So whenever we, for the rest of my presentation, talk about data going back and forth, we'll show these USPS boxes kind of traveling around, but really that's just a convenient way of representing computer packets traveling from one location to another.

Q. We're going to be talking a lot about encryption. It's an important aspect now in computer science. Could you describe what is encryption as it relates to network packets?

A. Absolutely. So encryption basically means that you don't want someone to necessarily snoop inside of your packet before it gets to you. So again, in our case, ESPN.com might not be something that we care about encrypting that data because it's just a video of a football game. On the other hand, if we're doing online banking, we don't want that data packet showing our balance, for example, to be intercepted by somebody and snooped inside of. So what people end up doing is they end up

encrypting the data so that even though you might understand where it's coming from or it's going to -- so the mailing label might still be visible to you -- what's actually inside of that packet is not visible. And that we just, here for convenience, representing with this padlock and the word Encrypted on it.

Q. So when you encrypt a network packet, you're locking away or encrypting the payload, the stuff in the box, but the mailing label is still publicly available, it's not kept secret; is that correct?

A. That is essentially correct. You are really not concerned about somebody knowing that the packet originated in Bristol, Connecticut and might be going, let's say, to me in Los Angeles, California. What I'm concerned with is that I don't want somebody to actually see inside of that packet. So I'm encrypting the payload, and the header information can stay on there.

Q. So how is information transmitted? You used ESPN from Bristol, Connecticut to a user on the west coast -- could you describe that process how packets are transmitted?

A. Sure. So in this case we would have a user who happens to be somewhere around Seattle and we have a server that's somewhere around Bristol Connecticut. So it turns out that ESPN is not a bad example, because that's where the headquarters is. And what the user will do is they will send -- they will click on the link on the browser, ESPN.com, and that will result in a

request packet being sent from the user's computer to the server that is owned by ESPN. At that point the ESPN server will slice up that video, for example, of the football game highlights into a large number of data packets, and it'll send them back.

What happens here is you have literally tens of thousands of these routers, these hockey pucks, distributed all over the place, all across the country, and they will decide how to route the data from one point to the next so that the original request arrives really efficiently from Seattle to Bristol, and the data gets returned also really efficiently from Bristol to Seattle.

And one thing I should stress at this point, we already mentioned this, even though just because PowerPoint was easier to create this way, this particular slide, and it shows a single path going from Seattle to Connecticut and back, in reality, any one of those routers could decide on the fly, dynamically, to reroute the packet and take any one of the other routes, meaning send it to any one of the other hockey pucks that we have here. So that the route one packet takes from Bristol to Seattle is not going to be necessarily the same as the route another packet takes. So all that stuff is determined on the fly by each router.

THE COURT: Is it necessary to have all those intermediate routers as opposed to just sending it directly from Connecticut to Seattle?

THE WITNESS: It turns out to be necessary, Your

Honor, simply because of the scale at which computer networks have to pass data around. Sending it directly would mean, would be the equivalent of a non-stop flight from Seattle to Bristol. So if you just think about how airlines operate, it is extremely unlikely that such a flight would exist because it would be very inefficient for the airline to move people around that way. So this is more of the, almost like the hub and spoke mechanism for routing things around so that you load up only those parts of the network that need to be loaded up in a given time, and the rest of the network can operate at optimal high speeds, for example.

THE COURT: Well, suppose you're sending it across the ocean? Does it go straight across or does it have to go through intermediate routers?

THE WITNESS: For that, this is -- I don't know if you have been reading about issues recently for example in South Africa. Their underwater cable fiberoptic cable was actually damaged, and the country had issues with high-speed connectivity to the rest of the world. What they do for that is they will have multiple of these literal physical cables that they will lay on the ocean floor, typically, that are very high-speed, where those cables will serve as kind of a single hop, once you get the data to one of those cables, a single hop to a very fast, very quickly transfer it to some router on the other side of the ocean.

THE COURT: Well, so does there have to be a physical connection between the various routers or is it wireless?

THE WITNESS: It can be wireless. It can be done through satellite, for example. But just like what we were advised to do for this particular trial, wired works much more reliably than wireless. There are various things that you cannot control in a wireless environment. So you can imagine both of these options being available, but if you want to control the throughput, the speed at which this happens, if you want to have those guarantees and if you want to go as fast as possible, wired is considered more reliable and generally faster in that sense than wireless.

THE COURT: Is it more secure?

THE WITNESS: That's the other thing. You can certainly, if you -- in a way, if you owned the wire, you can control who can access it. As soon as you get it into the ether, things get a lot trickier because who knows who is listening and snooping? Wired interaction is not entirely secure, there are certain reasons for that, but it's certainly a lot more secure in an average case than wireless interaction.

THE COURT: All right.

BY MR. ANDRE:

Q. So our ocean floors are littered with these large fiberoptic cables that transmit data from one continent to the other?

A. They are. And to be honest with you, I don't actually know how they do it. I know they use these huge ships and they have these spools of wire, but beyond that, how you ensure that these things don't get broken once they're on the ocean floor, I guess one way you find out they're broken is when it doesn't work anymore. So it's incredible technology that has existed for some time now.

Q. But once data transverses like from New York to London on the ocean cable, they get back into the router networks in Europe and in the United States?

A. Absolutely. From that point on it works exactly the same way. And as the Judge observed as well, there is data that can be transferred through the satellite links, for example, so in that sense wirelessly. But once it gets onto the network on the physical land -- in a sense when it starts going from servers on land to other devices -- that's where you can think of that network just a different map, but the same idea behind the network: These routers deciding how to figure out what the hops should be so that the data gets as quickly as possible from New York to London or New York to Moscow, for that matter.

Q. That kind of leads us into my next question about what is Cloud computing. We're talking about wireless and the Cloud, and it doesn't have to be wireless, I know, but could you describe -- when we hear Cloud computing, what are we talking about?

A. So Cloud computing is based on a very simple idea. Back 10, 15 years ago, most of us would have all of our data somewhere on a local hard drive, and then if we ran out of drive space on our computer, we might find external drives. So all of our videos of our cats, photos of our flowers, so on, all of that would be on a local drive. And eventually people realized that this is not efficient and not necessarily the best way of doing this for two reasons. One of them is every single one of us would have to keep buying these additional disk drives to store more and more stuff. Because we now have literally thousands of photos, every single one of us, and those take lots of space, for example. And lots of other data that we have as well.

The other reason is that if the local drive crashes, very often you lose some of this precious data. In this case we're showing a photo of a flower, and that might not be super-important to you, but you could imagine even things like videos of one's family from awhile ago could be important to you. And then you could imagine actual important financial data, for example, and things of that nature. So you wouldn't want that on the local computer necessarily for you yourself to maintain.

So what happened is companies like Amazon and Microsoft and Google and so on, they realized that they had these huge what they call server farms that can store lots and lots of data for

you, and they can also have -- since these computers are powerful -- they can do a lot of computing for you also if you wish them to. So what happens in today's computing most of the time is you will store these things like the photo of this flower somewhere on one of those servers. You may get, for example, free disk access with Apple or Google or whoever, and then whenever you want to access that photo or whenever anybody else, let's say your family or your friend, wants to see the photo of a beautiful flower in your garden, they send this request to essentially almost like an Internet link to this server, and that server is going to send that photo to your device.

So now what you're doing is you're doing all of this essentially on the Internet. So the Cloud itself is really the Internet. But the way the providers of the Cloud like you to think of it is a bunch of these high-powered servers that are completely hidden away from you and all you see is essentially almost like a remote disk drive, for example, from which you can access your data.

THE COURT: Well, the Cloud is really a collection of very large or high -- not necessarily physically large, but high-capacity electronic storage devices. Is that what it is?

THE WITNESS: That's correct, Your Honor. And also processing devices. So one type of Cloud service would be to store your data. Another type of Cloud service may be to do

some computing that is so expensive that doing it on your local device might be impossible. You might have to buy an incredibly expensive computer to do that with a very powerful processor. You can get it done for, let's say, you know, three dollars, some kind of nominal fee on Amazon, because Amazon happens to have a lot of spare computers, a lot of these computers that they have typically sitting around waiting for someone to use them.

THE COURT: They take up space somewhere, right?

Q. Amazon Web Service, that's the Amazon Cloud Service, don't they have like a very large building in Virginia and they have thousands and thousands of these computers? Could you describe what that looks like?

A. Yes. So one of my favorite photos that I saw, and it was a real surprise for me the first time, was this photo of, just like that Amazon building, a Google building with a bunch of what looked like yellow pieces of string. And it was these huge racks of individual computers placed in those racks, so literally thousands of them, and what looked like yellow string was really yellow Velcro. When one of those computers were to crash, to fail, for example, what they would do is just, they would just unsnap the Velcro, take it out of its housing and put another computer in, so that at all times they would have this huge bank of the computers available for hundreds of thousands of people, for example, to store their photos, to check their

email, to do web searches and so on.

All of these -- go ahead, please.

THE COURT: Well, if one of them crashed there's some sort of system that would save the data?

THE WITNESS: Yes. So all of this is highly replicated. They have different ways of ensuring that you as the end user, or I, would never notice that something went wrong. Computers crash all the time. There are a lot of different techniques that researches in distributed computing have developed over the past several decades to mask those types of crashes from the end user. If you have a single computer, a crash is quite definitive. There is nothing you can do about it. Your computer just crashed. If you have thousands of computers, it turns out that there are certain kinds of techniques that you can apply to -- even though you have a local crash -- to mask that crash from everybody except for the engineer who is in charge of ensuring that the network is at the, what they call a server farm, that it's functioning correctly.

THE COURT: All right.

BY MR. ANDRE:

Q. You mentioned --

MR. ANDRE: Go ahead, Your Honor. I'm sorry.

THE COURT: No.

BY MR. ANDRE:

Q. You mentioned a term there that I want you to drill down on. I know you wrote that back on software architecture. What is distributed computing?

A. Distributed computing is nothing more than any type of computing that requires more than one computer. So the moment that you have two computers talking to one another to do something, like for example the exchange of the photo of a flower, that's an incredibly simple example of distributed computing. One of them is sending a flower, a photo of a flower to the next one.

Then of course you have incredibly complex distributed computing systems. And anything that you do on the Cloud -- I mentioned Gmail, for example, everybody gets Gmail for free from Google. Every time you receive email or send email, that is distributed computing. Because what you're doing is you're sending it through the Google Cloud to whoever the recipient is. And of course you are likewise receiving the email. Any time you watch that video of football highlights from ESPN.com, that is an example of distributed computing. Every time you do online banking, and on an on. So every single instance when you have more than one computer that is required to do something, that's called distributed computing.

Q. Do most large companies build their systems on distributed computing today?

A. Nowadays I would say that probably an overwhelming majority

of all useful systems in the world rely on distributed computing.

Q. Let's change tacks a little bit here and let's talk about the technology regarding Centripetal's security patents that are involved in this case, the five patents in this case.

A. Yes. So these are the five patents, and Your Honor will be hearing a lot more about these over the next several days. Here I will just very briefly overview kind of at the core what these patents teach.

Q. Of the five patents, we'll be referring to them by the last numbers, the '193, the '806, '205, '856 and '176?

A. That's correct. I'll have a very simple slide kind of describing what each one of those five is, and I'll refer to them by the last three digits.

Q. Let's start with the '193 patent.

A. The '193 patent essentially deals with a set of rules that are applied at the level of routers and switches that decide whether a data packet that's coming through should be allowed to be forwarded on to whatever its destination may be, or it should be dropped. So you get a data packet, you inspect it very quickly, and depending on whether it matches one of these rules, you make a determination to forward it or drop it.

Q. When you say "forward" or "drop", what do you mean by that?

A. So when you forward the packet, essentially that means that what you're doing is you're letting it go from its source to its

destination. Dropping it means exactly what is shown here. What you're doing is you can think of taking that packet and putting it into a virtual trash can. So you do not allow it to continue.

Q. Let's go to the next patent, the '806 patent.

A. The '806 patent deals with preprocessing a set of rules. Once those rules are preprocessed, they're made available to the firewalls, routers and switches, then those rules are applied to the packets to examine the packets as they go through. And then at some point during this process you may want to update that rule set because you've discovered something new. You have some new knowledge and so on. And that new rule set needs to be substitutable for the original rule set without you really experiencing any issues with the network traffic. You can't expect things are just going to slow down because you're switching these rule sets or that you just drop packets while this switchover is taking place. In other words, you are treating this network traffic in exactly the same way, while within the router, switches and firewalls this action of switching these rule sets one for the other takes place in the background. And that happens in real-time.

THE COURT: Well, if you're putting in a new set of rules, you're supplementing the rules that are already there, I assume? You don't drop any rules, you're just adding them?

THE WITNESS: You are definitely supplementing the

rules, Your Honor, with, as I mentioned, if you have new knowledge, you may decide to drop a rule or eliminate a rule in the sense if, for example, you discover that your old set of rules was too permissive. So there might have been a rule that said allow all data from a particular server, then you discover that that server is not as secure as you thought it was, that rule may need to be eliminated and another rule put in its place.

THE COURT: All right. Instead of stopping everything from a particular source, you would just stop part of the material from a particular source? Is that what you're saying?

THE WITNESS: That could certainly be. I mean, there certainly could be --

THE COURT: Or you could just stop everything from --

THE WITNESS: Exactly. So I don't know if you've ever --

THE COURT: -- a particular source?

THE WITNESS: -- experienced a situation where you click on a link and, for example, your browser tells you this is an unsafe link and just blocks you from doing it, I don't know what the configuration in your courthouse is like in that regard, but that definitely happens. You can be completely blocked from accessing an entire website. Or you could be blocked from accessing certain content. So for example, the courthouse may allow an employee to go to ESPN.com, but because

videos require so much data, you can only read articles, you cannot transfer videos. That would be a very simple policy that ensures that whoever is a big football fan doesn't clog the network because they're downloading lots and lots of these very large videos from the server.

THE COURT: Okay.

BY MR. ANDRE:

Q. Go to the '205 patent. Describe what this patent is about.

A. The '205 patent is what I'm referring to as the Dynamic Security Policy packet patent. So essentially there is a Security Management Server that's involved, and that Security Management Server will send these security policies and will dynamically configure, while the system, the network is functioning, it'll dynamically configure the firewalls, the routers and the switches.

THE COURT: You mean by "dynamic" that it switches the rules while continuing to operate?

THE WITNESS: Essentially, Your Honor. The idea behind a lot of these systems that we're talking about here, this is what typically is referred to as 24/7/365 systems. That means they have to be up 24 hours a day, seven days a week, 365 days in a year. You can't bring them down. So what people have invented techniques for, in this particular case what Centripetal invented is a particular technique for dynamically configuring these various devices with security policies so that

you can, in fact, service the network without any slow-down, without losing any data and so on, while the network itself is running.

THE COURT: So you can change the rules while it's still operating?

THE WITNESS: Absolutely. Not only can you, but you have to. So the understanding is that, again, as we all gain knowledge, even in the real world, the rules of our lives change. And in computer networks, these rules could be updated for a variety of reasons, and everything still has to function, because there is an enormous amount of data just traveling around, so you have to figure out a way to change those rules and configuring these devices on the fly or, as they say in the vernacular, in real-time.

THE COURT: Well, do you hit the Pause button to change the rules or what?

THE WITNESS: Well, you can't quite hit a pause button, and you will hear more about these when these patents are described. But one of the things that you can do is, since computers are fast and doing these configurations with dynamic security policies or switching out rules and so on, as we talked about in the previous patent, that can happen very quickly. It doesn't happen instantaneously, but it happens very quickly. So what you can do, for example, and the patents talk about, is caching. So you cache the data temporarily, so you put it in a

special place when it's arriving, and as soon as the rules have been switched over or as the device has been reconfigured with the new policies, you quickly empty out that cache so you rapidly process that data and send it on.

THE COURT: Well, there has to be some pause of some nature while you're changing the rules. It may be done very rapidly, but I mean, there has to be some pause while the rule changes of some length.

THE WITNESS: And it's not -- yeah, it is not instantaneous. So what the patents do and what is commonly, relatively commonly done also in other distributed computer settings is you will -- since data is coming in, right, and for that short period of time, your router or your switch may not be available because you're changing these rules. So what happens in that case is you can think of it almost like taking whatever that amount of data is that is arriving while that switchover is happening, just store it on a local disk. And then as soon as the switchover happens, you grab that data and process it very quickly so that the recipient of the data doesn't perceive ever that there was anything happening with the network. So their impression is everything went on normally, but of course you as the owner of the network know that you did have that switchover of this dynamic configuration, and during that time all the data that was coming in, you were just storing it for a second and didn't do any processing on it, and then as soon as the new

configuration is in place, at that point you, in a sense, fire up the switch again, for example, and then you quickly reprocess that data and whatever else is coming in.

THE COURT: Okay.

BY MR. ANDRE:

Q. Let's talk about the '856 patent. Describe what we're looking at with that patent.

A. Sure. So this patent deals with that issue that we discussed before, which is that a huge proportion -- relatively large proportion of the network traffic today is going to be encrypted, meaning that you cannot peek inside the payload to see what's being sent around. And what that patent teaches is a way of dealing with the encrypted traffic and determining, based on a set of rules, whether that traffic, whether it's non-encrypted or encrypted. So it works for both types, whether it poses a threat and should be further inspected, and that's what this ramp or offramp, rather, that takes these packets up toward the top, whether they should be further inspected or whether they're not going to be a threat and they're allowed to continue on unimpeded to their destination.

THE COURT: Well, you would have to make that determination, I suppose, based on the source and -- it would have to be based on the source, wouldn't it, if you don't know what's in the packet?

THE WITNESS: One simple way of doing that -- you're

absolutely correct, that would be based on the source. So for example, if the source is untrusted, in a sense, that makes your job easy. Nowadays, the malicious agents or players on the Internet, they're more careful than that. So they will also sometimes co-opt legitimate servers to do their evil bidding for them, if you will. So in that case, in addition to looking at the source, you might have to inspect some other information. You might have to look at the timing of the packets, for example. You might have to look at or consider what other packets you may have seen previously so you can identify whether something strange is happening and so on. But you're absolutely correct: One way of doing this and one piece of information you absolutely need for something like this is where it came from, because the entire idea is you can't look inside the payload so you can't really know what that payload contains. Does it have a virus, for example? The idea is here you want to use other information to inspect the packet.

THE COURT: So you look at the source, plus timing, plus what else could you look at?

THE WITNESS: You can look, you can look at the source, you can look at the timing, you can look at previous packets that have arrived. You look at whether, for example --

THE COURT: Previous packets from the same source, I guess?

THE WITNESS: If that source for example, or previous

packets that suspiciously look like they might have -- let's say you keep getting packets that have identical sizes or packets whose encryption can be hashed to the same value. That basically means that whatever is encrypted inside of it is encrypted the same way and the data that's encrypted is identical. So that might be weird. Why are you getting essentially the same encrypted packet so many times? There are lots of different things, different --

THE COURT: Well, how do you know it's the same encrypted data? I mean, you wouldn't know that.

THE WITNESS: If for example -- so what you can do is, without peeking inside of the packet, the encrypted data is still -- if you think of regular data represented in a computer network as a bunch of ones and zeros. Encrypted data is still going to be a bunch of ones and zeros at the level in which it gets shipped around, except that to a human or a simple computer program, that bunch of ones and zeros is not going to be meaningful because it's some sort of a cipher. However, if that bunch of ones and zeros turns out to be identical across multiple different packets, for example, you would ask yourself the question of why am I getting copies of this same packet so many times, for example. So you don't know what's inside the packet, you just know that it looks weird. Sort of like getting a relatively small parcel but it's really heavy. That could be -- or getting a very large parcel and it's incredibly light.

That could be -- and this happens in a courthouse or if it arrives on Capitol Hill, for example, it might be a reason, might trigger some kind of rule that says, you know, this is atypical, let's figure out what's happened here.

THE COURT: Well, in other words, you can tell even though you can't look inside an encrypted packet, you can tell how much data is in it?

THE WITNESS: You can tell how much data is in it. That is correct. Because one of things in a header is -- so one of the things is which packet in the sequence it is, since this is going to be part of a larger chunk of data, so this is Packet No. 327, and then the other thing that it tells you, the header, that mailing label tells you is how large is the packet? So that's information that you can obtain in it. Of course if you can somehow divert this packet and check to see what else is happening, you can check, in fact, how large it is on your own. So you can keep it in some sort of secure environment, this offramp that we showed here, and poke around and figure out how big it is.

THE COURT: Well, you could get around that by just putting 25 percent encrypted -- or somehow it could be malware or whatever -- and then add 75 percent of gobbledegook to it and it would be look to be the same size, wouldn't it?

THE WITNESS: What you are describing is called obfuscation, and that's a --

THE COURT: Yeah, I run into that in court all the time.

THE WITNESS: Obfuscation is a technique that's sometimes used for legitimate purpose, but you're absolutely right, these malicious agents, malicious players on the Internet do those kind of things all the time where they try to disguise their evil intentions, if you will, by doing that kind of stuff. And there are also ways of uncovering that.

But one thing, just because -- just by me knowing that somebody's trying to obfuscate something, that already might trigger a level of suspicion. It might trigger a rule. You know, if you have nothing to hide, why are you obfuscating, essentially. So there are these techniques that you can apply, and some of those are -- some of this clever stuff is taught by the '856 patent.

THE COURT: Okay.

BY MR. ANDRE:

Q. Let's go to the last patent, the '176 patent.

A. Yeah, the fifth one in the sequence is, this is what we call, what I call a packet correlation patent. What it does is it essentially looks at packets that come in one way through a router or a switch, packets that go another way to a router or a switch, and it creates these logs and then tries to correlate these packets to try to figure out what, for example, is coming into the network is the same thing that's coming out of the

network and so on. So it tries to understand how these various data packets may relate with one another by inspecting these logs.

Q. Does it relate to trying to determine whether or not the packets are safe or not? Or secure?

A. That's one of the reasons you -- one of the important reasons you want to do this is because, you know, packets could be -- since you have this very open Internet, any place on the Internet, any router or any other device could be compromised, and it could do certain things to packets that make them dangerous, that change them in a particular way, that try to snoop inside of them, steal confidential data and so on. So what you want to do with something like this as you want to make sure that data has been unadulterated as it travels through a network.

THE COURT: So how is that different than dealing with encrypted? You can look inside the packet if it's not encrypted, right?

THE WITNESS: You are absolutely correct, Your Honor. The issue here -- you can do that. The problem becomes difficult when you consider that you might have billions and billions of these data packets, and you can't afford to look inside of all of them or even most of them because you're trying to make sure your network is as fast as possible. People want to, you know, they want to watch their NetFlix or whatever. So

in that case you develop these other techniques that can give you pointers to what might need to be inspected further, for example, where you might need to invest your resources so that if you can identify 98 percent of your traffic as being completely legitimate, you let it through very quickly, and then through these correlations of these log entries, if you can identify that four percent that is suspicious, you are allowing yourself to maintain this very high, extremely high network speed, and at the same time not miss potential issues with various security and data privacy concerns that you want to ensure.

BY MR. ANDRE:

Q. And for network security, is it important to have many layers of security and many different techniques to try to determine whether or not these packets that come through are legitimate?

A. Absolutely. It's just like any real-world situation where you are entering an environment that is, that needs to be secured, so that it's sensitive in some way, you are likely going to pass through multiple different layers of tests, and that's what happens in the computer network as well.

THE COURT: Well, if these particular packets that you check on, do you check on every 1,000 packets or do you check randomly? So many packets out of every 10,000? How do you decide which ones to check?

THE WITNESS: Right. So that's kind of the million-dollar question, and in some ways obviously you can't check every one of them. And if you take pick sort of a sampling you might get these, might build statistical models that tell you if you, for example, check every one thousandth packet you will have 99.7 percent assurance that nothing weird is going on. What this patent does is it tries to make that assurance even higher, because you may do your sampling, but here I'm also going to see if there are any tells. So for example, when somebody plays poker they might have a tell and that can tell you if they're bluffing or not. In this case, these tells could be this data packet coming in to this router had this particular signature, it had this particular information associated with it, coming out of the router it was changed. Why is that? So that could be a tip-off that you need to look at this a little bit more -- in a little more detail.

So for example, your Log Entry 1 and Log Entry 7, let's say, they're supposed to match up, and somehow they don't. And that triggers, subsequently -- it might trigger some additional action where somebody inspects that and makes sure that nothing strange or malicious is happening.

THE COURT: Okay.

BY MR. ANDRE:

Q. Well, let's talk about some of the products --

THE COURT: How much longer are you going to be,

Counsel?

MR. ANDRE: Just probably 15 minutes, Your Honor. Is now a good time for a break?

THE COURT: Yes, I think we ought to go ahead and take a break. It's approximately 20 minutes to 12:00. Let's take a recess until five minutes to 12:00. All right.

MR. ANDRE: Thank Your Honor.

(Recess taken from 11:39 a.m. to 11:57 a.m.)

THE COURT: All right. I believe we had just heard about a patent and we were going to a different subject?

MR. ANDRE: Thank Honor. May I proceed?

THE COURT: You may.

MR. ANDRE: Thank you.

BY MR. ANDRE:

Q. Dr. Medvidovic, we were just ready to talk about a very general discussion as to the accused products in this case, and let's start with the switches, or Cisco switches that are accused. Could you tell the Court what series of switches we'll be talking about over the next company?

A. These the Cisco Catalyst 9000 platform switches, and there are three different series of products we're going to be talking about in this case, the 9300, 9400 and 9500 series switches. They have a lot of different capabilities that Your Honor will be hearing about over the next several days. The one thing to point out is that these switches from Cisco, unlike the

traditional switches back in the day that we spoke about before, these switches actually have integrated security capabilities in them.

Q. So we take -- when you say the different series, the 9300 the 9400 and the 9500, why are there different numbers for these switches?

A. They may have different capabilities. So one of them, for example, the 9400, it's called stackable, so you can put them on one another. Another one might be available in the Cloud and so on. So their individual sets of features might not be identical, but the core capabilities they do are those of switches, and then with this idea of integrated security on the inside.

Q. Do they all use the same operating system or software for the purposes of this trial?

A. Yes. I was going to mention this when we talked about the routers. It's not just switches, but when we talk about the next set of technologies as well, they use the same key software that runs everything on the switch. This is the -- it's known as the operating system.

Q. Lets' go to Cisco's routers then.

A. Yes. So this is, again, these are -- so you think of the switches as that equivalent of that telephone operator switchboard. Routers are more like the ambulance dispatchers. And there are three different series of products, the 1000

series aggregation services routers, the 1000 series integrated service routers, and the 4000 series integrated services routers. And they are Cisco's -- so they're -- these are the actual boxes that these products are built as, but they are the equivalent of these hockey pucks that you see in the upper right-hand corner in the background. And so the thing to point out is that although they might have slightly different capabilities, their purpose is to ensure in the network high performance, reliability, and also integrate security, and all of these routers run the same operating system software across the various families or the various series, and it's also the same software that is run on Cisco's switches as well.

Q. Now I want to talk about something Cisco refers to as their Digital Network Architecture. They call it DNA for short. We'll just refer to it as the Digital Network Architecture. What is the Digital Network Architecture in Cisco's system?

A. So this is an architecture that basically is in charge of network management. So it does things like configure your network, troubleshooting it and so on. And it interacts with the routers and the switches, and we'll see that in a diagram in just a second.

Q. In the paragraph describing the Cisco DNA center, it says "Provision and configure all of your network devices in minutes." What does it mean to provision, in computer science, a network device?

A. So essentially make it available. So you can set it up to use it for whatever purpose it is set up for. So in this case this would be provisioning routers and switches, and that means that after they have been configured by the Digital Network Architecture, or DNA, they are then capable of being used in the network and doing the job that they were made to do in the first place.

Q. Then the next sentence "Advanced Artificial Intelligence, AI, and machine learning."

THE COURT: With all due respect, Counsel, I think we ought to have the witness's picture on the big screen instead of yours.

MR. ANDRE: Okay.

THE COURT: I don't know how to do that.

MR. ANDRE: When he talks, Your Honor, he'll come on. When I ask the question it jumps over to me.

THE COURT: I know. Well, it's been on you while he's talking. It's not switching over.

MR. ANDRE: Dr. Medvidovic, could you say something and maybe get me off the screen?

THE WITNESS: Yes, this --

THE COURT: Okay. Go ahead.

THE WITNESS: It's a setting on Zoom. I hope it's been fixed, Your Honor.

BY MR. ANDRE:

Q. So when the next paragraph talks about "Uses Advanced Artificial Intelligence and machine learning to monitor, troubleshoot and optimize your network", what is artificial intelligence and machine learning in computer science?

A. So these are ways of having the computer or router, in this case the software, in a way learn in a similar fashion to how a human does. So you basically would observe what's happened in the past and then based on what it has seen in the past, it builds, in a way, a model, which is really nothing more than an expectation of what should be true in the future. So it essentially tries to, among other things, predict, based on what it has seen, what it's likely to see. And given that information and that knowledge that it has, it can make some decisions that, let's say 10 years ago, might have taken some time to figure out, but in this case this is all kind of happening in real-time so that these intelligent decisions can be made without slowing down the network.

THE COURT: Such as learning which packets to inspect, for example?

THE WITNESS: For example, Your Honor. So it definitely would learn that packets coming in one part of the network tend to be, let's say, more suspicious. It might also learn that data tends to cluster around certain times of the day. So in North America, for example, between 1 and 6 a.m., the amount of network traffic may go down, but then you will see

peeks, for example, during a work day, and it might decide that additional monitoring might be need to be done during those times or additional resources or computers or more servers might need to be dedicated to it and things like that. So it can do a lot these kinds of intelligent decision-making. Of course it's all done in the software, which is why it's called artificial intelligence, but in some way it is intelligent.

BY MR. ANDRE:

Q. Does it require intelligent feeds or threat intelligence feeds to work on different security?

A. In order for you to do anything with what's referred to as advanced artificial intelligence, and especially machine learning, you need to have a lot of information. So this intelligence has to come from somewhere. And the way you like to think about it, the way that computer scientists talk about it, basically, what you get is a lot of data available in a network for example. The data is, in a sense, it's naked. It doesn't really have anything meaning behind it. So you need these facilities to actually turn that data into information, and that information is what's actionable. That information is what becomes your intelligence based on which you can build these models to adjust the network to do various things with different data that's traveling from various places and so on.

Q. We turn to the next product offering, the StealthWatch product. Could you generally describe the StealthWatch product?

A. So the StealthWatch product essentially provides the ability to collect various kinds of security analytics, and it does prediction of advance threats. So things that might not be readily obvious as being malicious, StealthWatch is actually able to discover those threats. It does so with the help of a couple of other technologies that we'll talk about in just a second.

Q. And just for a bookmark in that, what are the other technologies that StealthWatch works with?

A. So StealthWatch works with Cognitive Threat Analytics, which we'll talk about briefly in a second, and Encrypted Traffic Analytics. So a lot of the network drive is encrypted, and there is this particular technology that Cisco has that deals specifically with that kind of data.

THE COURT: Now, there were two categories you said, encrypted data and what was the other one?

THE WITNESS: The first one was Cognitive Threat Analytics -- and I will show a slide for each one of them, Your Honor, in just a second.

So Cognitive Threat Analytics, Cisco's acronym is CTA, and Encrypted Traffic Analytics, they refer to as the acronym ETA.

THE COURT: Well, let's not use acronyms --

THE WITNESS: Yes.

THE COURT: -- at least at this stage until I learn

what they are.

THE WITNESS: The only reason I mention it is because these slides would have gotten really busy, so on the next couple of slides you will see those two acronyms, but I will spell them out as I speak about them.

BY MR. ANDRE:

Q. When we go to the next slide regarding Cognitive Threat Analytics.

A. Cognitive Threat Analytics does various things like monitoring like if you have unwanted applications on your computer or somewhere on your network. It turns out that you may think, well, how could I possibly have an unwanted application, I only have things that I installed? Turns out that it's possible to get these things sort of surreptitiously installed on a machine so that they watch what's happening, for example, steal one's data and so on.

You can also -- Cognitive Threat Analytics also monitors data ex-filtration, meaning somebody somehow trying to get the data that is local and belongs to you somewhere to a remote location so they can look at your private information. It also monitors for things likes security breaches, for example. So it does various things that are part of this larger StealthWatch technology.

Q. So the ex-filtration is when the data is sitting on your computer and someone's trying to steal it as opposed to

infiltration?
A. Exactly. So they basically find a way of getting to whatever sensitive portion of your hard disk is and start siphoning that data off without your knowledge and quietly sending it to some other remote location. This actually happens all the time. So technology like Cognitive Threat Analytics deals with that type of issue.
Q. Go to the next product offering, the Identity Services Engine. What is that?
A. Identity Services Engine basically ensures that you can have access to your network, to your resources, from wherever you are. So this is -- and it's trusted access. And this is why it also has this symbol with the fingerprint. It provides network-based security regardless of what the actual physical location is from which a user is trying to access that data.
Q. And the next one is the Encrypted Traffic Analytics?
A. The Encrypted Traffic Analytics is also a thing that goes with StealthWatch, although as we'll see in a slide or two, it gets also placed on, for example, Cisco's switches, and it deals with being able to track and analyze this encrypted traffic without actually having to decrypt it. Decrypting is expensive. First you have to figure out how to do it; in other words, what the cipher is, and also doing that whole process can take a lot of time. So what Encrypted Traffic Analytics does is it does this tracking and analyzing based on this other information that

we spoke about, Your Honor, before the break: Things like where it's coming from, how often it arrives, what its size it, where it might be heading and so on. It uses that kind of information to track it and analyze it and figure out what might be going on on the network.

THE COURT: Well, it doesn't -- actually it can't look at what it's not supposed to see, it just has to use other sources or functions to try to figure out what may be in there. Well, they can't figure out what may be in there, they can figure out whether it should be blocked.

THE WITNESS: Exactly. And very often, very often you don't necessarily care what's inside of it *per se*. The important information to you is, is this dangerous? That is what -- that's something that's actionable.

THE COURT: Okay.

BY MR. ANDRE:

Q. I notice in the slide there it says it's a component of switches, routers, the Digital Network Architecture and StealthWatch. Is this just like a solution or software sitting on all these different devices?

A. Yes. And when we -- I think we have a slide coming up that has this kind of more complete picture of what a Cisco-enabled architecture may look like. So you will see this yellow button -- I'm sorry, orange button with ETA on it in various places because this software ends up playing roles in all of

these various parts of the different switches and routers.

Q. You're looking at encrypted traffic as prevalent in all these different spaces?

A. Absolutely. Because encrypted traffic is so prevalent in computer networks today, you have to account for it in all kinds of different settings and scenarios when you're trying to ensure your network's reliability, performance and security.

Q. Let's talk about the Cisco's firewalls that are involved in this case.

A. There are five different sets of firewall products. What they call the Cisco ASA 5500 with Firepower, ASA stands for Adaptive Security Appliance. These are actually Cisco products in the upper left-hand corner. These are firewalls that are getting phased out, but the other four series of firewalls, the 1000, 2100, 4100 and 9300, these are Cisco's Firepower firewalls at issue in this case and that are still being actively worked on by Cisco.

Q. Are these Firepower series, are they the follow-on to the ASA firewalls?

A. Yes. They provide some services that are similar -- or the same and some other services that are innovations, obviously, just like a technology company would introduce them to their new products.

Q. Let's go to the Firepower Management Center. Can you describe what that is?

A. Sure. The Firepower Management Center is -- and again, this is the symbol of the firewall that we used before on the left-hand side with the brick wall, but you will see the same flame symbol in Cisco's own schematic, if you will, logo and for the Firepower Management Center or the FMC at the top of this diagram. And it basically does things that a firewall, you would think that the firewall would do; things like managing your network at that particular point in the network, protecting against malware, checking and blocking attempts at malicious intrusions into your network and things like that.

Q. Let's show a slide how the switches are integrated into a network with Cisco's system. Could you describe how it's set up?

A. Sure. So what you see at the center of this diagram is one of the Cisco switches. And all of the switches work in essentially the same way. So you can imagine any one of the three different series of switches that we talked about before working the same way. And what it does is this particular switch enables the interaction of those two computers and those two printers. And what it does is, on it, it has this Encrypted Traffic Analytics. That's the ETA button. It communicates with the Digital Network Architecture, which is -- it has the DNA symbol. And then the Digital Network Architecture also has its own copy of Encrypted Traffic Analytics. The switch also interacts with StealthWatch. StealthWatch has both the

Encrypted Traffic Analytics, which is the orange button, and the Cognitive Threat Analytics, which is the purple button.

And StealthWatch, in addition to talking to the switch, it communicates with the Identity Services Engine, and then the Identity Services Engine itself, this fingerprint button with the blue color and the letters ISE in it. So the Identity Services Engine also interacts with the switch. So there is quite a bit of functionality put together to enable Cisco switches to provide some of these security and network analytics types of functionalities that we talked about before.

Q. Is this an example of the distributed computing that you were talking about earlier?

A. It absolutely is. Not only are there different services provided by Cisco itself, for example, the Identity Services Engine has to communicate with the software that runs on the switch itself, but of course the switch by definition enables distributed computation because you now have these two computers and these two printers and they can see, mostly operate, with one another seamlessly. So you can pick one printer if you want to print a document on, or you could have one computer access information, send email, communicate in whatever other ways with the other computers.

Q. Let's show how the Cisco products interact with routers. The next line.

A. So if this particular figure looks similar to the figure,

that's because it is very similar. Routers, of course, enable these small sub-networks that are connected by the switches to be connected in larger networks, which we spoke about before. So this is one example of a Cisco router in the middle, that gray box, and on it, again, just like with the switches, the router itself has the Encrypted Traffic Analytics. And then I mentioned this before, both the routers and the switches run the same operating system, and their capabilities are very similar when it comes to things like threat analytics and security and so on. So what you see on the bottom, the bottom left of this figure are the same exact technologies, the Digital Network architectures, StealthWatch, the Identity Services Engine, the Encrypted Traffic Analytics, the Cognitive Threat Analytics, that's exactly the same as we saw on the switches of the previous slide.

Q. Let's see what the Cisco firewall products look like in a network.

A. So on the right-hand side, at the top of the slide you have the router and the switches that we talked about before. And then in the middle now you have a Cisco firewall product. It's one of the five products that we discussed that are part of this case. And that firewall product interacts with the outside network, so this server shown on the left-hand side. And of course on the right-hand side is the protected part of the network, so whatever the firewall itself protects. And to

ensure whatever security capabilities it has, it has to interact with the Firewall Managing Center, which is the circle that has that flame symbol on it, and that provides all that firewall management and malware protection and prevention of intrusions and so on.

Q. If we go back to the slide that you showed the basic network structure earlier, now could we superimpose on that slide how Cisco's secure network interacts with the basic network?

A. Yes. So again, just to keep in mind that this is a very simplified view of what the computer network may look like, because it only has a couple switches and one router and one firewall, and a real network will have hundreds and thousands of these things. But Cisco's technology that we just discussed maps to this picture in the way that is shown here. There are these technologies or solutions that Cisco provides, the Firepower Management Center which provides the threat intelligence to Cisco's firewalls, and the Identity Services Engine and StealthWatch and the Digital Network Architecture with two different software capabilities or technologies. The ETA, which is Encrypted Traffic Analytics, and CTA, which stands for, again, Cognitive Threat Analytics, so the orange and purple button, even though they're kind of grouped just because it's a single slide overlapped over the top, all of them apply to both the routers and the switches. Again, I think it's important to

stress that because Cisco's routers and switches share that part of their, key part of their software.

And then of course the Encrypted Traffic Analytics also resides -- a copy of it, if you will -- also resides on all of Cisco's switches and Cisco's routers. So when you kind of compose it all together, you get this relatively complex picture of a network that does a whole bunch of different things.

Q. We have the threat intelligence coming down from the Cloud into these systems making, what was dumb before, smart systems, what is threat intelligence?

A. Threat intelligence is essentially that actionable information that we talked about before; the thing that results from huge amounts of data being observed and information being extracted from them and then being built into these models of what might be happening in your system. So that intelligence is what is actually actionable to the firewall, routers and switches so they can not only be highly efficient, but they can also provide the level of security that Cisco in this case intends them to have.

MR. ANDRE: Thank you, Dr. Medvidovic.

Your Honor, that concludes our tutorial unless you have any questions for Dr. Medvidovic.

THE COURT: Okay. The term "threat intelligence", that means what the system would detect that would cause it to change its rules; is that correct?

THE WITNESS: That is certainly one thing that it might do. Just like any in the real world, when people collect intelligence on another country or another company, some things may be immediately actionable. And in the example Your Honor just brought up, it might result in you changing the rules. Other things you might just elect to kind of sit and watch. So some of the intelligence could be relevant, you know, two hours from now, for example. Even though right now you have that information, what it applies to has not occurred yet, in a way. And part of this advanced artificial intelligence and machine learning that we saw in that one slide from one of the Cisco technologies, part of that is this ability to try and predict what you might see. What a computer might see in the future. So certainly some of it is actionable immediately -- you know, this is bad, block it, act on it right now -- and the rest of it could be something that you should watch out for based on what has been seen in the past.

THE COURT: Okay.

THE WITNESS: In a way when you --

THE COURT: So it creates what we might describe as artificial intelligence that enables the system to either act on it or put it in a category of something to watch out for?

THE WITNESS: Essentially. And it also allows the system to possibly predict what's going to happen on the network in the future so that it can more intelligently or more

efficiently provision its resources. So some of these models could actually tell you how the network is likely to behave in some respect at some point in the future based on this intelligent predictive capability from what they call, again, advanced artificial intelligence and machine learning.

THE COURT: All right.

THE WITNESS: So the way I liken this to the real world, if one watches a movie that involves, for example, spies, then you might hear somebody say "We've picked up a lot of chatter." Immediately that chatter, for example from a terrorist organization, that chatter might not be immediately actionable, but it gives them pause. It makes them listen for it more, and watch what else might be happening.

THE COURT: All right. Thank you.

Does that complete your presentation, Mr. Andre?

MR. ANDRE: It does, Your Honor. We'll turn it over to Cisco to let them give their tutorial at this time.

THE COURT: Okay.

MR. GAUDET: Thank you, and good morning, Your Honor. Matt Gaudet on behalf of Cisco. Our tutorialist will be Dr. Kevin Almeroth. And there is Dr. Almeroth. Just be sure that he has control of the slides before we begin the proceeding.

COURTROOM DEPUTY CLERK: Mr. Almeroth?

THE WITNESS: Yes, ma'am?

COURTROOM DEPUTY CLERK: Would you please raise your right hand?

KEVIN ALMEROTH, having been duly sworn, was examined and testified as follows:

MR. GAUDET: Thank Your Honor. Dr. Almeroth will present a tutorial that will cover some of the same ground, and perhaps some of them overlap, we can go through a little bit quicker, but then we'll also offer some additional points that we think are important as you face the various issues in this case.

With Your Honor's permission, may I proceed?

THE COURT: You may.

MR. GAUDET: Thank you.

TECHNOLOGY TUTORIAL OF DEFENDANT

BY MR. GAUDET:

Q. Dr. Almeroth, would you introduce yourself to the Court and tell the Court about some of your background qualifications to give this tutorial?

A. Sure. My name is it Kevin Almeroth. I've been a professor in the department of computer science at the University of California at Santa Barbara for about 23 years. Before that I spent nine years at Georgia Tech. I got a Bachelor's, a Master's and a Ph.D all in computer science with an emphasis on networking. So for the last 30 years or so I've been working in computer network technology, computer security and Internet

technology.

MR. GAUDET: Thank you. If we go to the next screen there, Dr. Almeroth?

Your Honor, we've broken this tutorial into four basic segments. This presentation structure is up on the screen. And what we plan to do is go one by one through these four modules, if you will, and at the end of each, we'll stop for a summary and to be sure that if there are any other questions that you hadn't had a chance to ask, that we want to obviously be certain that we're responsive to anything.

THE COURT: All right.

BY MR. GAUDET:

Q. The first module is just the basics of networking. Sort of how the Internet works. Dr. Almeroth, will you give the Court a tutorial on the basics of networking?

A. Yes. And I will do my best not to cover the same ground. What I will do is where I have slides that overlap, I'll just indicate that there's an overlap there, likely just move on if there are no questions.

I think that where I start my tutorial is a little bit different than Dr. Medvidovic. I start off with the Internet as a cloud. The idea is that the Internet is large, it's complex, it spans the entire world. So to start to understand some of the technology of the patents and accused products, it's important to treat that Internet as an onion, try and peel back

some of the layers.

The first place that I want to start with, the idea that the Internet really connects an array of businesses and different kinds of users. For example, you'll see companies that provide content, things like Amazon, NetFlix, Google. Zoom is on here, right? Without the technology of the Internet and the technology of these content-providing companies, we wouldn't be able to do this trial today.

In large part, those businesses that are providing content using the Internet do so to a fairly broad array of users. They could be users in their individual homes, there can be small business networks, large business networks, government networks. And some of these networks that connect through the Internet span hundreds of nodes or thousands of different computers.

So the next kind of step to understand how all of these different devices are connected together is to look at what's inside of the Internet, sort of its core or sometimes what's called its backbone. And the analogy that I would draw here is Dr. Medvidovic used the idea of the phone system. And it's very similar in the sense that if you have one user who connects to the Internet through EarthLink, it might be possible they want to send an email to somebody who is at the courthouse. So there needs to be a mechanism through this core of the network, through this backbone of the network. So I have a slide, Slide 6, that breaks down that Internet into a set of different

service providers. So the idea is that the Internet is really a network of networks; meaning you have lots of different service providers who are all connected together, all of whom have customers. Those customers are connected to other customers, and probably the analogy of either the Post Office or the phone system works, right? But if I want to send a letter to somebody in Italy, it will be on the United States Postal Service for some portion of that trip, and then it will convert to possibly the UK or go directly to Italy. But the idea is all these different networks cooperate together to connect all of the users with all of the different businesses to exchange data the world over.

Now --

BY MR. GAUDET:

Q. If I could interrupt just to ask you a clarifying point so that the Court sort of sees the correspondence between this and what Dr. Medvidovic did. Do you recall the slide that had the United States and about two dozen routers and someone at ESPN in Connecticut over to someone in Seattle, Washington? Do you recall that?

A. Yes.

Q. Would those routers -- and it was represented there as a couple dozen routers -- would those appear in this big cloud? Is that sort of the reference of that network of routers that gets things from one point to the other?

A. That's right. All of these different networks are composed of routers, and those routers work to move the data that's being communicated around the network. I'll go back to the Post Office analogy, right? If I put a letter into the mail, it gets carried to my local post office, then they sort it, they decide where it should go, and maybe it goes to the central facility in Los Angeles and maybe it gets put on a plane and flown across the country to Washington, D.C., and then you would look it the headers in the packets and try and decide where this data should be routed. So the concept of routing data in the Internet is not really new, it's kind of borrowed from other analogies. But the idea in the Internet with all of these different providers is that data gets passed around in different routers and it's the routers that decide what to do so the packets can go from their source to their destination.

Now, in order to enable all of this kind of communication there's a series of standards that are used in the Internet.

THE COURT: Let me ask you a question.

THE WITNESS: Yes, sir.

THE COURT: Why do you have NetFlix, FaceBook, Amazon and Google outside of the Cloud and those other four entities inside of the Cloud?

THE WITNESS: Excellent question. So the entities outside of the Cloud aren't really considered to be in the network. They are, in fact, running their own networks. They

connect to this Internet, the Internet, in order to send their data to users. So think about this again from the Post Office analogy. The Post office analogy is worldwide, it consists of a lot of different countries. They would be in that center cloud in the middle. Now, companies or people would send letters to each other and it would arrive into the Post Office as soon as you put it into one of the blue boxes or dropped it off in the mail slot. Companies can do that as well. So they use the same infrastructure.

Now in the Internet you have different called service providers like EarthLink, Verizon, AT&T and Cox. They're the networks whose business it is to connect users and businesses together. So it's through their networks that they connect users to data. So for example, EarthLink makes money by charging people to connect to their network, and then it receives data from those users and delivers it to whatever the destination would be. And so there's slightly different kinds of businesses and service providers to the companies that provide the content to the user.

THE COURT: Okay. So if they're outside the Cloud, they either supply or receive content and if you're inside the Cloud you just circulate it?

THE WITNESS: That's right. You're a transit provider. So for example there are companies -- you asked this question of Dr. Medvidovic, that there are companies that manage

the undersea cables that go from California to the Pacific Rim, from the East Coast to the UK. So they make money by deploying that infrastructure, charging companies that want to deliver their content over those particular cables.

One of the things that was kind of impressive is obviously the Internet as a network of networks has to work worldwide through all sorts of different countries and languages. And it does so based on standards. It does so using protocols. The specific ways of communicating the exchange of data. I think it's relevant for the purposes of this case to point out that one of the important standards organizations is call the IETF, Internet Engineering Task Force. And they developed many of the standards that relate to the Internet. Those standards are called Requests for Comments. It's a little bit of a historical acronym, but that's what the standards are called. So a common protocol like IP or HTTP have standards that are published --

BY MR. GAUDET:

Q. Dr. Almeroth, I'm going to stop you there only because you used a acronym before saying what it meant. So if you could, before you -- even if it's just an example, it's probably a good thing just to be sure you actually say it out.

A. Yes, sir. Was it IP or HTTP? Okay. So IP is the Internet Protocol. HTTP is the Hypertext Transfer Protocol. HTTP is used in web pages to transfer data over the web, and then IP is

really one of the building blocks that allows data to use the web.

All right. With that, again, I want to go back to the Internet as a Cloud. And this is also, I think Dr. Medvidovic talked about the idea of the Cloud for computing and storing. Again, there are companies that would connect to this Cloud and that's why it's called Cloud computing or Cloud storage.

THE COURT: Okay. Well, that last slide you showed me just illustrates that there is -- not this one, but the one after that -- it just shows that there's a organization that establishes protocols for how information is going to be circulated. Is this an international protocol?

THE WITNESS: It is.

THE COURT: Okay. Who determines the protocol?

THE WITNESS: There are meetings of this organization, and different people who wish to contribute to these standards will show up at these meetings and they will make suggestions about what the rules should be for what these standards should look like.

THE COURT: Is this an international body then?

THE WITNESS: Yes, it is.

THE COURT: So everybody, all the countries join together to establish an international protocol? We don't have different protocols in every country, it's one protocol that applies internationally?

THE WITNESS: That's correct. And many of the companies who sell products, it's in their interest to make sure that these standards are well understood and easy to deploy so that there's no confusion. So for example, companies like Cisco participate in some of these organizations. I as a researcher have written some of these Requests For Comments standards. I've published them at the IETF and have become standards that are in use. So it's countries and companies and researches, all who are trying to define the way the Internet should work for the best interests of the Internet.

THE COURT: Is this a non-profit organization?

THE WITNESS: It is.

BY MR. GAUDET:

Q. Dr. Almeroth, to round that out, is that why, for example, manufacturers that are operating on their own can build equipment knowing that, if you send something on a piece of Cisco equipment, for example, and it gets received by a competitor's piece of equipment, they can still be sure they're going to be able to communicate with each other?

A. That's correct.

THE COURT: Okay.

A. I mean, there's other standards organizations, obviously, for non-Internet standards. They define what the voltage is, what plugs will look like. There are all of those kinds of standards for the Internet as well, and many of them come from

the Internet Engineering Task Force.

THE COURT: Okay.

A. Okay. Moving on to Slide 8., one of the things I've done is kind of shrunk the Internet down, because I want to give a few examples of kinds of networks that users or businesses might use to connect to the Internet? And so the first one I'd add is kind of a small fairly simple network, and it shows three users on different kinds of devices. So this might be a kind of network like what's in my house. So you'll have User 1 is a personal computer, and User 2 on a laptop, 3 on a tablet. And those computers would connect to a gateway or a router. I think Dr. Medvidovic talked about switches and routers and briefly described what those are. Essentially those kinds of devices allow somebody in their house to then connect to their service provider. So if I have Verizon service at home, I would use one of these routers to connect my home network to the Internet. So I would have a phone connection or some sort of connection that would then connect it to the Internet.

Q. Dr. Almeroth, in this image before we move on to the next one, in addition to the word "Router" there, it also says "Gateway". And what's the significance of that word, "Gateway"?

A. Right. The one concept I will discuss in more detail later is that, when you have a network of networks, there's usually a boundary between one network and another network. My network and my neighbor's network. The courthouse's network from the

law office's network. So there's boundaries. And usually at the boundary of one of these networks is a gateway. And this will become important when it comes to security because, as I'll show, that within a network I might trust all of the people that are in my house, but when I go out into the Internet at large, I'm exposed to hackers and people who want to steal my data, then that portion of the network will be untrusted. So you'll see, for example, around the three users in my house, a little box. So that indicates kind of my network separated from the rest of the network. Even though I can connect to it, I try and protect the computers in my network from somebody on the outside of the network.

THE COURT: Well, you're connected to the Internet by paying somebody to connect you, right?

THE WITNESS: Yes, sir.

THE COURT: And that person doesn't provide any security for you unless you buy it independently, do they? I mean, unless you pay extra to get security.

THE WITNESS: Exactly.

THE COURT: So anything that you've got on your network, whether it's at your office or your home, can be observed by anyone else unless there's some security between you and the Internet?

THE WITNESS: Yes, sir. That is absolutely correct.

THE COURT: Okay.

BY MR. GAUDET:

Q. Dr. Almeroth, just to maybe put one final point on that. You recall the device, the firewall discussion from Dr. Medvidovic? The third major device called the firewall?

A. Yes.

Q. Just using this very simple example, where would the firewall in this image go if we were to include the firewall?

A. It could go one of, actually, several different places. You could have a firewall that sits between the gateway, router and the Internet as a separate -- sometimes it's called an appliance. Like a separate device. You could include a firewall inside of the gateway or the router itself. Dr. Medvidovic said that that traditionally hasn't been done. I actually think it's been done for at least a couple of decades.

You could also put additional protections or firewalls further into the network. Maybe not in my home, but in a more complex business network you might have additional firewalls and other routers in the network.

THE COURT: In other words, the person you pay to connect you could also pay to provide you security which would, if it was at that site, it would protect anybody who subscribed to their services, I guess?

THE WITNESS: That's correct. And that's -- I think Dr. Medvidovic described multiple lawyers. I have a slide later on that talks about defense in depth: The concept that you can

have multiple layers of security, you can pay multiple different kinds of companies to provide security in different ways. You could have passwords on your computer that would prevent people from accessing data. That will become very important in this case.

THE COURT: All right.

BY MR. GAUDET:

Q. If you would proceed with your explanation, Dr. Almeroth?

A. Yes. So I have two additional builds on Slide 8, and the whole point of these two additional builds is to introduce some additional terminology really to get at the point that they're networks with increasing complexity. So in the lower left I've added Network 2. I've now added routers and switches inside of that network. I have additional users. And then in the lower right-hand corner of that box that's labeled the Server. So now this might be more like a business or it might be a government office. So this business now has a server that it wants to make available, potentially, to the public, the information on that server that users can then request from either in that network or outside that network.

Q. Dr. Almeroth, again, just a point, just to be sure that we're all on same page about what a server is as opposed to other kinds of computers, what sort of information, for example, might be kept on a server somebody might want to have access to?

A. It might be entertainment. So for example, it could be a

movie or an electronic book. It could be, say, the courthouse where the courthouse makes documents available to the public, or rulings. So those documents would be stored on a server and then designated for access by the public. I think consistent with the discussions we've had on security, it could certainly get much more complex.

THE COURT: Well, you could put on the server some sort of security.

THE WITNESS: That's right. You might have --

THE COURT: I just had a case that involved case filings and court rulings being made available to the public, but then you also have documents that are filed under seal, and I suppose you could put on the server some sort of software that would prevent such documents from being made available to the public while other documents were. The server could serve as a place to put security, is that accurate?

THE WITNESS: Absolutely. Absolutely. And I think your intuition serves you well, that you were starting to sense just how complex networks can be and how much demand for different types of security in different places. And in fact this third build-out shows it an even more complex network. And now what you see is you might even be able to take portions of your network and say the servers on this portion of the network, kind of lower half of Network 3, are things that can be accessed by the public through that gateway, but Users 1, 2, and 3 at the

top are on a private network inside the courthouse. There's no reason for anybody outside of the courthouse to be accessing those computers. So you can put in security gateway, routers along the path, the servers, the user computers, lots of different places and lots of different types of security.

THE COURT: Well, I could write a draft of an opinion that would only go to User 1, 2 and 3, or User 1, 2 or 3.

THE WITNESS: That's correct.

THE COURT: And that way the public couldn't see the draft. Then when I issue the final opinion you send it down to the bottom and it's accessible to the public. In other words, they can't see the drafts, they can only see the final opinion.

THE WITNESS: That's correct. And so if you go to your network administrator and say the courthouse network should be set up this way, that person has the responsibility of figuring out what kind of commercial products should be used to implement that kind of security. It's a hard problem.

THE COURT: But there's a path from the lower section to the top section. Why do you have a path there if Computers 1, 2 and 3 are only going to get certain information and people at the bottom get -- or vice versa, actually, in this case?

THE WITNESS: Well, when you're finished drafting that opinion and you're ready to release it, that opinion has to get on the server at the bottom. And so you will use a pathway from your computer to publish that decision on that server. Now it

turns out that that pathway between those layers needs to be protected very carefully to not allow somebody to infiltrate your network by using that path. So there's security to be implemented between those two routers to monitor that path very closely.

BY MR. GAUDET:

Q. Dr. Almeroth, just in terms of the timing that you're talking about, you know, the notion of having various kinds of security on routers and switches that are inside of the network, is that something that just came about in the last few years or has that been around for a while?

A. No. I've got a couple of slides, but kind of the key point is that when the Internet really started having e-commerce, when there were businesses selling things on the Internet, people were exchanging credit card numbers, that really happened in the mid- to late '90s. So computer security and network security really started to take off about 25 years ago. Even over the last 15 years, a lot of these problems have been exposed and dealt with by commercial offerings.

Q. Unless the Court has further questions, if you would proceed?

A. Yes. So what I wanted to do is I wanted to take this Network 3 and isolate it as you see here on Slide 9. I'll come back to this slide to really show some of the next set of core concepts that I want to go into. You see the title of the slide

is called an Enterprise Network. So an enterprise like a business. And again, the point I would have made here but I I've already made in part, is that it's this whole network that has to be managed by, say, the network administrators for that organization. So if this were, say, the courthouse in Norfolk, the administrators of this network wouldn't just trust the people in the Internet to do the right thing. So you build security into the network to protect that network from outside people who would attempt to misuse it.

So the idea of an enterprise or sometimes called a domain, is really an enclave or a protected domain in which computers can be protected as a group.

Q. Dr. Almeroth, when you refer to sort of the administrators of the network, you mean for example what we sometimes call the IT person who actually knows how everything works so that people like me who just want to see the computer on can do that, and they'll take care of the details?

A. That's right. IT staff, usually if it's got more than a few switches and routers, it's going to be more than one person. But yes, the IT staff.

All right. The next concept I want to get across I think is one that we've covered in some detail. So I'll probably go through the next set of slides more quickly.

The first is an animation that really just shows that you can send packets between users and you can send packets from

inside of the network to outside of the network. This slide introduces the concept of a packet. Dr. Medvidovic introduced that concept. It's really the idea that instead of exchanging, say, large files like the movie or the document, if it's made available on the Internet, it's divided up into these small pieces of data called packets. So the packets will flow around the network through the routers between sources and destinations. So the concept of a packet is one that I want to expand on in a little bit of detail.

Now, the other point that I would make is I showed a couple of simple examples of data packets. The reality is kind of Slide 10 shows that you can imagine that on a network there's thousands if not millions of packets flowing around that network per second. So in the course of trial already, the tutorial already, there have been millions and millions of packets being exchanged among all of the different participants. So you can imagine, once you expand out of this enterprise network, the network at large, that there are billions and trillions of packets exchanged throughout the entire world. It's through all of these protocols, these rules for communication, that facilitate the delivery of data. So part of what is going to happen and part of what we need to secure is these packets being delivered through these routers.

When Dr. Medvidovic used the analogy of a packet being a package with a label on it, I have a very similar animation. We

talked about headers and payloads. I think that that's an accurate description of a packet. The header is equivalent to, say, the address information on the outside of an envelope. Just like on an envelope, there are rules for where you put information and what structure that information should have. You have two-letter state abbreviations. Five- or nine-digit zip codes. The return address goes in the upper left or at the top on the back of the envelope. So there's agreements and protocols and formats to what all these things should look like, and in large part that's what's goes into the header of a packet. And just like the information on the letter, it's used by routers to decide where to send those packets so that they reach a particular destination.

Slide 11 shows you some of the types of information that can be in a header. I mentioned protocols. Internet Protocols, IP. The Transmission Control Protocol, TCP, then HTTP.

THE COURT: The transmission what?

THE WITNESS: The Transmission Control Protocol. It's one of the protocols that's used in the Internet to deliver data. The point that I would make here is that often headers have multiple protocols in the header at the same time. To sort of foreshadow where this is going to go, you can envision a security device looking at some of the different protocols in the header to determine whether or not something is malicious or not. So the point on this slide is really to show that there

could be a fair amount of complexity, detail, about what's in the payload and where the packet came from, where it should be going.

THE COURT: What's in the payload or what's in the header?

THE WITNESS: Both. In some cases the header will provide an indication of what's in the payload. It will tell you -- the header will tell you that you have a web request. It will tell you that this packet is part of a set of packets.

So the additional two points here is that one of those pieces of information is what's called an IP address, and that's like the street number, and the street, city, state and zip code on a letter. If you've ever seen one of these kinds of numbers, it's kind of four numbers separated by periods. And that's the numbered address that computers on the Internet will have. You'll see, if you looked into a computer network, numbers like that representing the header's path.

THE COURT: Well that would be like my Internet address --

THE WITNESS: Yes, sir. Exactly.

THE COURT: -- would be an Internet protocol.

THE WITNESS: That's correct.

THE COURT: And it might be sent to a number of people, not just the one person.

THE WITNESS: You would need multiple addresses. Each

person you would send it to would have their own IP address in their computer. So you would have to send -- you could send it multiple times from your computer or send it to someone who would then make copies and then send it on.

THE COURT: Well, you can have -- I mean, your computer can have something in the software that automatically sends it to all of the judges in the court, for example --

THE WITNESS: That's correct.

THE COURT: -- or --

THE WITNESS: And your software will say for these judges this is the IP address of their computers and will do all of the work for you to divide that document up into a series of packets and put those onto the network or into the network.

THE COURT: Okay. I think this might be a good stopping point. It's time for our luncheon recess. We're going to have to interrupt your testimony, the question is is this a good time to do it?

THE WITNESS: Any time is a good time for lunch, Your Honor.

THE COURT: Well --

MR. GAUDET: Your Honor --

THE COURT: -- depends on what kind of diet you're on. I'm on a diet.

MR. GAUDET: Your Honor, based on the presentation, I think this is a perfectly fine place to take a break and all get

some lunch.

THE COURT: All right. Well, let's resume at five minutes after 2:00.

MR. GAUDET: Thank you, Your Honor.

THE COURT: All right.

(Luncheon recess taken at 1:04 p.m.)

\- - -

CERTIFICATION

I certify that the foregoing is a true, complete and correct transcript of the proceedings held in the above-entitled matter.

Paul L. McManus, OCR

Digitally signed by Paul L. McManus, OCR
DN: cn=Paul L. McManus, OCR, c=US, email=pmcmanusocer@verizon.net
Date: 2020.08.10 10:28:14 -04'00'

Paul L. McManus, RMR, FCRR

Date